CLAIMS

1. An enciphering method comprising the steps of:

enciphering data with a first key; and

enciphering said first key with each of a plurality of predetermined second keys.

2. An enciphering method according to claim 1, wherein said data includes at least one of key information, documents, sound, images, and programs.

3. A recording medium having information items recorded thereon, said information items comprising:

first information obtained by enciphering data with a first key; and

second information obtained by enciphering said first key with each of a plurality of predetermined second keys.

4. A recording medium manufacturing method comprising the steps of:

obtaining first information by enciphering data with a first key;

obtaining second information obtained by enciphering said first key with each of a plurality of predetermined second keys; and

recording said first and second information on the same recording medium.

5. A deciphering method comprising the steps of:

inputting first information obtained by enciphering data with a first key and second

information obtained by enciphering said first key with each of a plurality of predetermined second keys;

deciphering said first key using at least one of said second keys to obtain said first key;

determining by a specific method whether or not the obtained first key is correct; and

deciphering said data using said first key after the determination to obtain said data.

6. A deciphering method according to claim 5, wherein said data includes at least one of key information, documents, sound, images, and programs.

7. A deciphering device comprising:

input means for inputting first information obtained by enciphering data with a first key and second information obtained by enciphering said first key with each of a plurality of predetermined second keys;

storage means for storing at least one of said second keys; and

deciphering means for deciphering said first key from said second information inputted from said input means using at least one of said second keys in said storage means, determining by a specific method whether or not the obtained first key is correct, and deciphering said data from said first information using said first key after the determination to obtain said data.

8. A recording and reproducing device comprising:

reading means for reading first information and second information from a recording medium on which said first information obtained by enciphering data with a first key and said second information obtained by enciphering said first key with each of a plurality of predetermined second keys have been stored;

storage means for storing at least one of said second keys; and

deciphering means for deciphering said first key from said second information read by said reading means using at least one of said second keys in said storage means, determining by a specific method whether or not the obtained first key is correct, and deciphering said data from said first information using said first key after the determination to obtain said data.

9. A key control method comprising the steps of:

causing a first caretaker to take custody of a plurality of predetermined second keys;

causing a second caretaker to take custody of first information obtained by enciphering data with a first key and second information obtained by enciphering said first key with each of said predetermined second keys; and

causing a third caretaker to take custody of at least one of said second keys.

10. A deciphering device comprising:

reading means for reading first information, second information, and third information from a recording medium on which said first information obtained by enciphering data with a first key, said second information obtained by enciphering said first key with each of a plurality of predetermined second keys, and said third information used for key determination have been stored;

storage means for storing at least one of said second keys;

first deciphering means for deciphering one of the enciphered first keys selected in the order determined from said second information using one second key selected in the order determined from said second keys stored in said storage means, determining on the basis of said deciphering result and said third information whether or not said first key obtained by said deciphering is correct, and repeating said selection and said determination until the first key determined to be correct has been obtained; and

second deciphering means for deciphering said data from said first information using said first key said first deciphering means has determined to be correct.

11. A deciphering device according to claim 10, wherein:

said third information is information obtained by enciphering said first key with said first key itself;

and

when the key obtained by deciphering one of said second information using one of said second keys stored in said storage means coincides with the key obtained by deciphering said third information using the former key, said first deciphering means determines that the former key is the correct first key.

12. A deciphering device according to claim 10, wherein said data includes at least one of key information, documents, sound, images, and programs.

13. A deciphering device comprising:

a first unit built in a driving unit of a recording medium or connected to the driving unit of said recording medium without the CPU bus of a computer, including:

means for transferring first information obtained by enciphering the data read from said recording medium with a first key, second information obtained by enciphering said first key with each of a plurality of predetermined second keys, and third information used for key determination in such a manner that at least said second information and third information are transferred safely without being externally acquired; and

a second unit connected to said first unit via the CPU bus of said computer including:

means for receiving said first information,

second information, and third information from said first unit via the CPU bus of said computer in such a manner that at least said second information and third information are received safely without being externally acquired;

storage means for storing at least one of said second keys;

first deciphering means for deciphering one of the enciphered first keys selected in the order determined from said second information using one second key selected in the order determined from said second keys stored in said storage means, determining on the basis of said deciphering result and said third information whether or not said first key obtained by said deciphering is correct, and repeating said selection and said determination until the first key determined to be correct has been obtained; and

second deciphering means for deciphering said data from said first information using said first key said first deciphering means has determined to be correct.

14. A deciphering device according to claim 13, wherein:

said third information is information obtained by enciphering said first key with said first key itself; and

when the key obtained by deciphering one of said

second information using one of said second keys stored in said storage means coincides with the key obtained by deciphering said third information using the former key, said first deciphering means determines that the former key is the correct first key.

15. A deciphering device according to claim 13, wherein said data includes at least one of key information, documents, sound, images, and programs.

16. A deciphering device comprising:

reading means for reading first information, second information, third information, and fourth information from a recording medium on which said first information obtained by enciphering a third key with a first key, said second information obtained by enciphering said first key with each of a plurality of predetermined second keys, said third information used for key determination, and said fourth information obtained by enciphering data with said third key have been stored;

storage means for storing at least one of said second keys;

first deciphering means for deciphering one of the enciphered first keys selected in the order determined from said second information using one second key selected in the order determined from said second keys stored in said storage means, determining on the basis of said deciphering result and said third information

whether or not said first key obtained by said deciphering is correct, and repeating said selection and said determination until the first key determined to be correct has been obtained;

second deciphering means for deciphering said third key from said first information using said first key said first deciphering means has determined to be correct; and

third deciphering means for deciphering said data from said fourth information using said third key obtained by said second deciphering means.

17. A deciphering device according to claim 16, wherein:

said third information is information obtained by enciphering said first key with said first key itself; and

when the key obtained by deciphering one of said second information using one of said second keys stored in said storage means coincides with the key obtained by deciphering said third information using the former key, said first deciphering means determines that the former key is the correct first key.

18. A deciphering device according to claim 16, wherein said data includes at least one of key information, documents, sound, images, and programs.

19. A deciphering method comprising the steps of:

reading first information, second information, and

third information from a recording medium on which said first information obtained by enciphering data with a first key, said second information obtained by enciphering said first key with each of a plurality of predetermined second keys, and said third information used for key determination have been stored;

deciphering one of the enciphered first keys selected in the order determined from said second information using one second key selected in the order determined from said second keys, determining on the basis of said deciphering result and said third information whether or not said first key obtained by said deciphering is correct, and repeating said selection and said determination until the first key determined to be correct has been obtained; and

deciphering said data from said first information using said first key determined to be correct.

20. A deciphering method comprising the steps of:

transferring first information obtained by enciphering the data read from a recording medium with a first key, second information obtained by enciphering said first key with each of a plurality of predetermined second keys, and third information used for key determination from a first unit built in a driving unit of said recording medium or connected to the driving unit of said recording medium without the CPU bus of a computer to a second unit via the CPU bus of the

computer in such a manner that at least said second information and third information are transferred safely without being externally acquired; and

in said second unit, deciphering one of the enciphered first keys selected in the order determined from said second information using one second key selected in the order determined from said second keys stored in said storage means, determining on the basis of said deciphering result and said third information whether or not said first key obtained by said deciphering is correct, repeating said selection and said determination until the first key determined to be correct has been obtained, and deciphering said data using said first key determined to be correct.

21. A deciphering method comprising the steps of:

reading first information, second information, third information, and fourth information from a recording medium on which said first information obtained by enciphering at least a third key with a first key, said second information obtained by enciphering said first key with each of a plurality of predetermined second keys, said third information used for key determination, and said fourth information obtained by enciphering data with said third key have been stored;

deciphering one of the enciphered first keys selected in the order determined from said second

information using one second key selected in the order determined from said second keys, determining on the basis of said deciphering result and said third information whether or not said first key obtained by said deciphering is correct, and repeating said selection and said determination until the first key determined to be correct has been obtained;

deciphering said third key from said first information using said first key determined to be correct; and

deciphering said data from said fourth information using said third key obtained.

22. A deciphering unit device that receives information via the CPU bus of a computer from a bus transfer unit built in a driving unit of a recording medium or connected to the driving unit of said recording medium without the CPU bus of the computer and deciphers data on the basis of the information, said deciphering unit device comprising:

means for receiving first information obtained by enciphering the data read from said recording medium with a first key, second information obtained by enciphering said first key with each of a plurality of predetermined second keys, and third information used for key determination from said bus transfer unit via the CPU bus of said computer in such a manner that at least said second information and third information are

received safely without being externally acquired;

storage means for storing at least one of said second keys;

first deciphering means for deciphering one of the enciphered first keys selected in the order determined from said second information using one second key selected in the order determined from said second keys stored in said storage means, determining on the basis of said deciphering result and said third information whether or not said first key obtained by said deciphering is correct, and repeating said selection and said determination until the first key determined to be correct has been obtained; and

second deciphering means for deciphering said data from said first information using said first key said first deciphering means has determined to be correct.